Req 2. The AM **must** provide an interconnection interface to its distribution network at points where all of the ISP's traffic aggregates.

Req 3. The AM **must** create and maintain network element configurations that implement the IP transport classes offered to the ISPs.

Req 4. The AM **must** route consumer traffic to and from their chosen ISPs so that each ISP can manage IP address space for its service and route service-bound IP traffic for its customers. The AM will either separate consumer IP traffic destined for different ISPs, or provide mechanisms to allow ISPs to implement access controls.

Req 5. The AM **must** provide a DHCP service from which CMs acquire their IP configurations and RFC868 Timeservers which modems use to acquire the current time-of-day.

Req 6. The AM **must** provide TFTP servers to host configuration files that correctly configure modems for the services they are entitled to.

Req 7. The AM **may** allocate non-Internet routable addresses to the consumer PC **if** the ISP POI is inside the AM distribution network. However, **if** the ISP POI is made outside the distribution network and Consumers' tunneled packets leave the AM's Head end systems the Consumer PC **must** be given a routable IP address.

Req 8. The AM **must** provide a connection point for the ISP within the bridged network.

Req 9. The PBR **must** be the first-hop router beyond the consumer PC if the AM implements Policy-based routing to separate consumer traffic.

Req 10. Essential network services such as DHCP, Time, TFTP, SNMP, and Syslog **must** be available to the modem. DHCP service **must** be available to the Consumer PC so that it can obtain its address in the IP transport space. The AM **must** accept all packets destined for the consumer's ISP interconnection.

Req 11. The AM **must** provide periodic traffic reports for each IP transport class to each of the ISPs that use that class for service delivery. The ISPs **must** provide estimates of customer growth to the AM for purposes of capacity planning within each of the IP transport classes.

Telcordia Technologies, Unrestricted Access.
Copyright © Telcordia Technologies, Inc.

2 The Testing Network

The testing network is designed to facilitate rapid construction of testing scenarios. The network contains bridge and router-based CMTS units and routed and bridged segments. A headend interconnect that aggregates all traffic interconnects the CMTS-coaxial plant to systems that supply required network services and act as service provider systems.

2.1 Assumptions

2.1.1 Cable Modems Are Bridges

CMs are operating as transparent bridges rather than routers. A router or hub may be connected to the CM-CPE interface.

2.1.2 CMTS Aggregation Devices

CMTS can function as an Ethernet Bridge or IP Router. Tests illustrate the different configuration requirements for each type of device.

2.1.3 DOCSIS

The scenarios in this document are based on the DOCSIS standard, but are not intended to test the DOCSIS standard itself. DOCSIS equipment is required here because of its configuration capabilities and increasing deployment in cable plants. No testing of non-DOCSIS CMTS or CM equipment is performed, or implied by the testing reported here.

2.1.4 Number of ISPs

The testing scenarios assume there are at least two ISPs that can be accessed by Consumers. This is approximated in the test network through multiple Internet-reachable links with independent address spaces.

2.2 System Configurations and Access Scenarios

The testing network consists of five CMTS units manufactured by Nortel, 3Com, and Cisco. Each CMTS is configured with (at least) one downstream transmitter and from one to 6 upstream receivers. The downstream frequency of the Cisco and 3Com units is at IF 44Mhz and is shifted to a higher frequency using General Instruments' C6U upconverters. The upstream and downstream signals are mixed in a diplex filter and the unsplit portion of that filter is used to feed a coax-only distribution network to the cable modems. The testing network is illustrated in Figure 4.

The CMTS unit's Network Side interface is 100BaseT. Each CMTS NSI is connected to one of two 100BaseT hubs which divide the units into networks, one bridged and the other a routed network. The routed network has a Cisco 4000 between the hub and the headend interconnect. AOL(2)001799

Telcordia Technologies, Unrestricted Access.
Copyright © Telcordia Technologies, Inc.

The headend interconnect consists of a Redback SMS 1000 that aggregates all of the traffic coming from the CMTS/coax distribution/CM network. The headend interconnect has a local network on which the network services and CM configuration (TFTP) systems are located. There are two egress points from the headend interconnect to nodes that serve as the service provider systems. One terminates in a WinNT 4.0 system that serves as a PPTP tunnel endpoint.

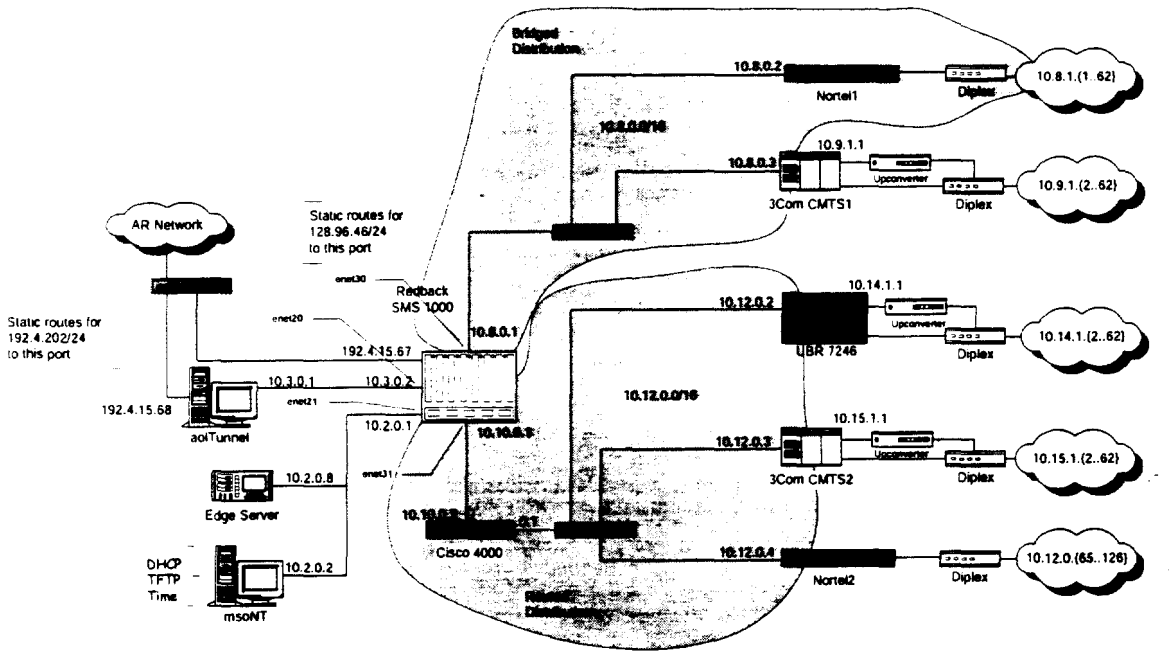

Figure 4 Test Network and Services Design

2.3 CMTS Configurations

2.3.1 Nortel CMTS1000 (2 systems)

- 1 downstream transmitter with integrated upconverter,
- 4 upstream receivers,
- 100BaseT Network Side Interface

2.3.2 3Com Total Control system (2 Cable Access Routers)

- 1 downstream transmitter at IF
- 2 upstream receivers
- 100BaseT NSI

2.3.3 Cisco uBR 7246

- 1 downstream transmitter at IF
- 6 upstream receivers

AOL(2)001800

Copyright © Telcordia Technologies, Inc.

- 100BaseT NSI

2.4 Test Configurations

The test configurations are arrangements of network elements, components, and software that permit testing of different system configurations in light of the Equal Access requirements. The distinction between routed and bridged network designs has been made before. In either type of network it is possible to connect and configure CMs to have unlimited access to internetworking services. Providing for differentiated service offerings, based on either the PC being used for access, or specific user identity is more involved. The Equal Access requirements only specify separation of traffic from consumer PC to service provider. This involves moving all service-bound traffic directly from Consumer PC to service provider, and preventing traffic from moving to places it is not permitted to go to.

Two technologies have been identified to maintain traffic separation, tunneling and policy routing. Tunneling creates a virtual point-to-point network between 2 tunnel endpoints. This allows remote endpoints to be directly connected to the hosted network and obtain all of their services from that network. Three tunneling technologies were investigated, PPTP, L2TP, and PPPoE. PPTP and L2TP are end-to-end protocols and proved to be easy to implement and use. PPPoE requires a bridged network and due to limitations of the firmware in the head end interconnect was complicated to deploy.

Policy routing does not create a virtual transport space. This is important because of the need to create and manage subnets to many segments of the networked system. Physical network topology must be overlaid with many address spaces if each ISP is to manage address space for its customers. Not all internetworking services are available in such an overloaded network, thus causing operational and management difficulties as the system and subscriber base scale up.

The following networks correspond to the six configurations identified in Table 1.

2.4.1 Routed Distribution Network, CMTS is Router, Tunnel Access

This configuration represents the case where the CMTS is a router (Cisco uBR 7246) and the distribution network contains multiple routers (Cisco 4000, Redback SMS 1000). The target ISP system is the ISP Tunnel server. The tunneling software is Microsoft Dial-up Networking with the iVasion PPTP/L2TP client.

Telcordia Technologies, Unrestricted Access.
Copyright © Telcordia Technologies, Inc.

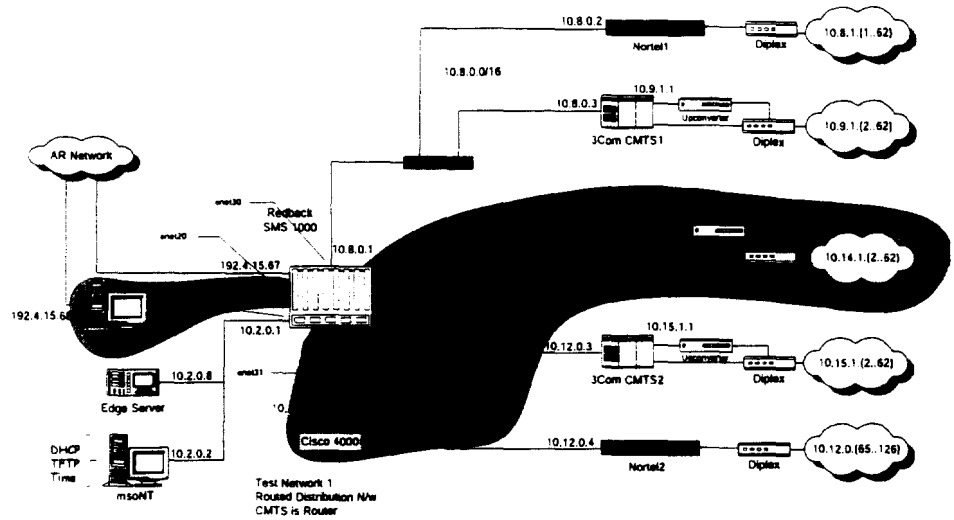

Figure 5 Test Network 1 Routed distribution, CMTS router, Tunnel Access

Default Gateway is 10.14.1.1.

2.4.2 Routed Distribution Network, CMTS is Bridge, Tunnel Access

This configuration (Figure 7) is very similar to the previous network. There is 1 less router hop (the CMTS is not a router hop) between the Consumer PC and any destination. See Figure 6 for an example.

Default Gateway is 10.12.0.1.

```
C:\lcn_data>tracert 10.14.1.2

Tracing route to 10.14.1.2 over a maximum of 30 hops

  1   15 ms   16 ms   16 ms  10.2.0.1
  2  <10 ms  <10 ms  <10 ms  10.10.0.2
  3  <10 ms  <10 ms  <10 ms  10.12.0.2
  4  <10 ms   15 ms   16 ms  10.14.1.2

Trace complete.

C:\lcn_data>tracert 10.12.0.65

Tracing route to 10.12.0.65 over a maximum of 30 hops

  1   31 ms   15 ms   16 ms  10.2.0.1
  2  <10 ms  <10 ms  <10 ms  10.10.0.2
  3  <10 ms   15 ms  <10 ms  10.12.0.65

Trace complete.
```

Node on Routed CMTS Network

Node on bridge CMTS

Figure 6 Distance traces through different CMTSs, same Distribution Network

Modems and PCs acquire addresses in the bridged network (10.12.0.0). The cable-facing port on the Cisco4000 is configured (ip helper-address) to relay DHCP broadcast requests (DHCP-DISCOVER) to the DHCP server (10.2.0.2).

AOL(2)001802

Copyright © Telcordia Technologies, Inc.

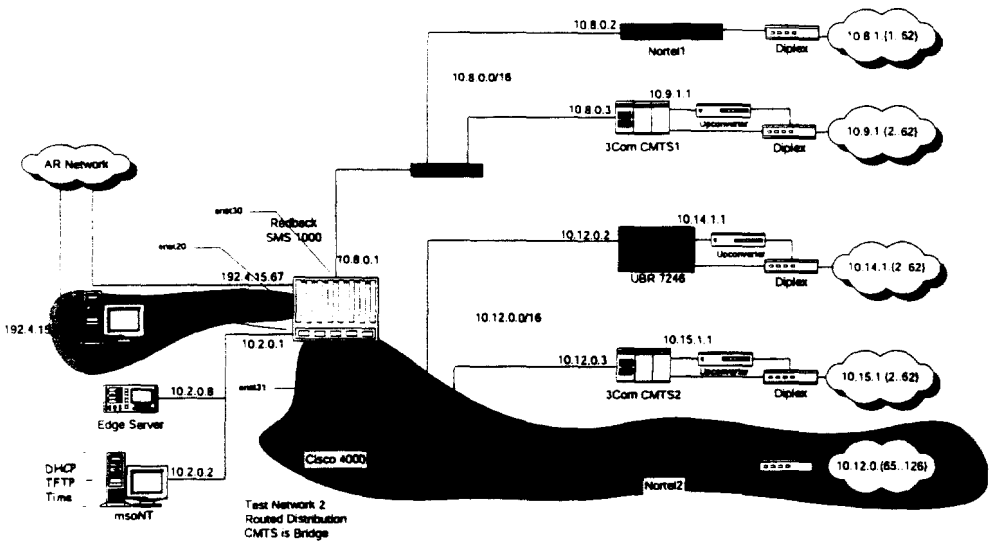

Figure 7 Test Network 2: Routed distribution, CMTS bridge

The CMTS, all CMs, and PCs connected to this network all are in the same address space. The default gateway is the first hop router, at 10.12.0.1.

2.4.3 Bridged Distribution Network, CMTS is Bridge, Policy Access

This configuration is the same as that of Section 2.4.4 with the SMS1000 acting as the policy router. CMs are given non- Internet routable addresses as usual. However, this requires the PCs - in the same network - to be given non-routable addresses as well. This limits their ability to reach internet destinations. This is overcome by using another physical port that is bound to the overlaid address space, tied to the same bridged network.

2.4.4 Bridged Distribution Network, CMTS is Bridge, Tunnel Access

Tunnel access in a bridged network is possible using PPPoE or one of the Layer 3 tunnel solutions (PPTP or L2TP). The PPPoE implementation in the SMS1000 requires the Ethernet port to be set up to carry encapsulated traffic. CMs do not create PPP-encapsulated frames so the multiple port tie-in must be employed if PPPoE is the tunnel technology in use. In this case, one port is encapsulated and the other is not[1].

[1] This limitation is removed with Redback AOS V3.1, available for general release in 1Q 2000.

Telcordia Technologies, Unrestricted Access.
Copyright © Telcordia Technologies, Inc.

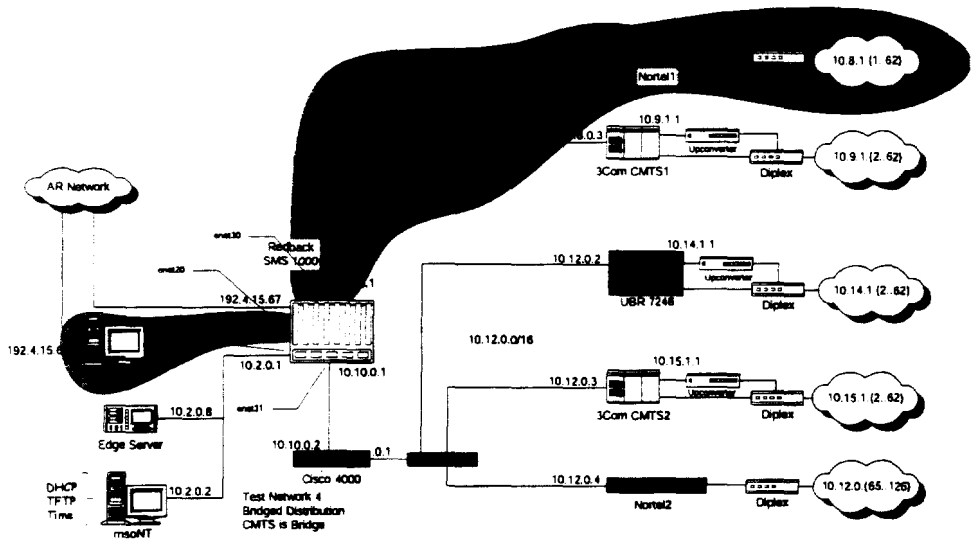

Figure 8 Test Network 4: Bridged distribution, CMTS Bridge

Tunneling through this configuration using L2TP or PPTP works as expected.

2.4.5 {Routed, Bridged} Distribution Network, CMTS is {Bridge, Router}, Policy Access

The tested configuration is Routed distribution, bridged CMTS. The router next hop (Cisco4000) eliminates the need to use two physical ports on the SMS1000. This network configuration uses the SMS1000 as the policy router. Policies were implemented in the Cisco4000 using route-map groups. CMs used DHCP to acquire their addresses in the normal fashion. The PCs representing customer of ISPs were assigned addresses from the appropriate spaces. The tested configuration is illustrated in Figure 9.

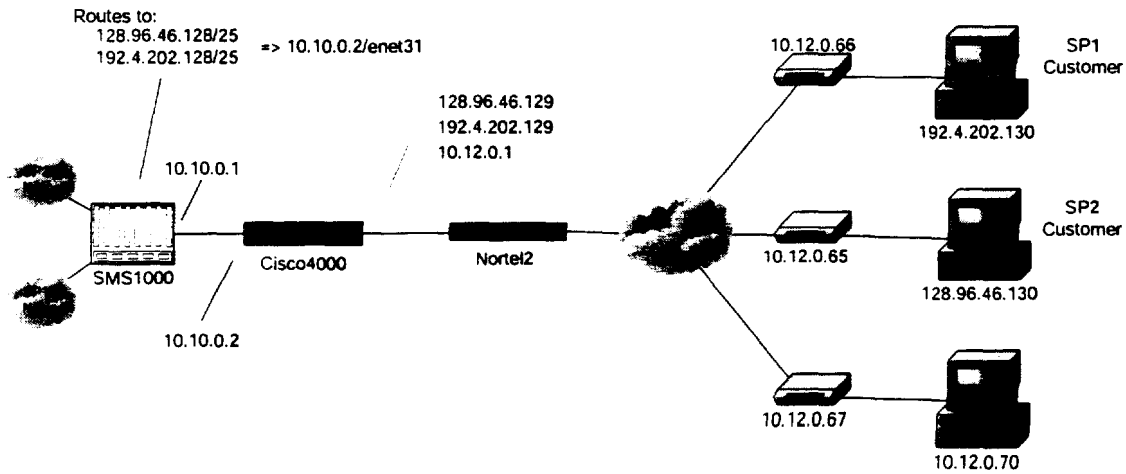

Figure 9 Policy Testing Network

AOL(2)001804

Copyright © Telcordia Technologies, Inc.

The SMS1000 configuration places the policy definition on the incoming interfaces and directs packets to their respective ISPs based on the source address. The configuration and illustration can be found in Appendix B -.

2.4.6 Bridged Distribution Network, CMTS is Router, Tunnel Access

This configuration is easily managed with the end-to-end tunnels providing the necessary separation of address spaces.

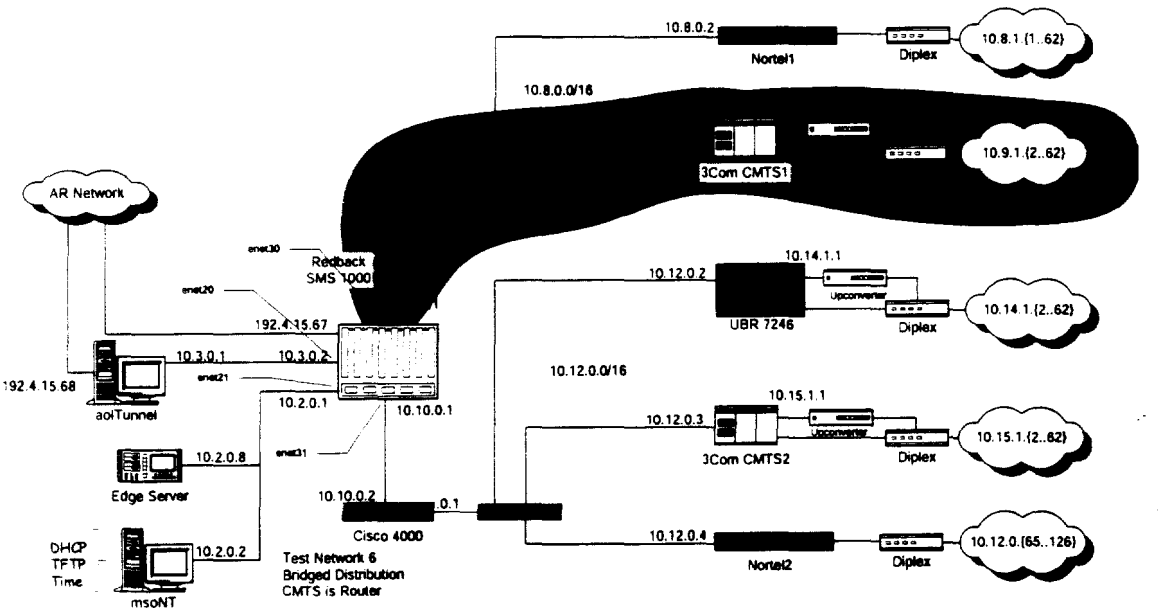

Figure 10 Test Network 6: Bridged Distribution, CMTS router

2.5 Service Configurations

The test network runs single instances all of the required network services. The network services machine is configured as follows:

WinNT 4.0 SP5, Pentium 166Mhz, 40 MB RAM, 1.5GB Hard Disk Storage.

DHCP - Microsoft DHCP service on Win NT 4.0 Server

TFTP - Nortel LCN TFTP service on Win NT 4.0 Server

Time - Nortel LCN Time service on Win NT 4.0 Server

2.5.1 Transport Address Pools

The DHCP service in use (Microsoft) allows address pools to be created for " scopes" - an aggregate of common parameters - based on the subnet of the node that is requesting a configuration. Within a scope, different clients can be identifed by their Ethernet MAC address. Some CMTS units are capable of distinguishing between DHCP-Discover requests for modems and PCs, but this feature is not universal and not used in our testing.

AOL(2)001805

Copyright © Telcordia Technologies, Inc.

Each subnet that contains a CMTS has a 10.X.Y.Z/16 subnet allocated for modem and PC addresses. Figure 4 indicates the complete address plan. All network elements involved in routing decisions have been configured with static routes.

2.5.2 DOCSIS Configurations

CM configuration files determine what kind of transport classes and to some extent what services can be accessed by a Consumer. The test environment primarily uses four CM configuration files for testing.

Unrestricted, Universal access file - This configuration has a low bitrate class of service, no privacy enabled and will work with any CM-CMTS combination. This configuration is shown in Figure 11.

```
// Dump of bronze.cm Generic CM configuration file.

Bay Networks .MD5 Dump Utility - v1.1
NetworkAccess = Yes
ClassOfService =
    ClassId = 1
    MaxDownstreamRate = 256000
    MaxUpstreamRate = 32000
    UpstreamChannelPriority = 0
    MinUpstreamRate = 0
    MaxUpstreamBurst = 4260095
    PrivacyEnable = 0
CM-MIC = c5bfc825a329a9dcf895c80dbdbc3808
CMTS-MIC = 4083ac4a28de166f646699ef64768571
CM MIC is valid.
```

Figure 11 Generic, no-frills CM configuration

Unknown Modem Configuration - This consists of a low bit-rate Class of Service and IP packet filters that permit only access to the network services systems. This configuration allows modems to acquire an IP address, configure, register, and pass traffic from an attached PC.

See Appendix A1 for the full text.

Provisioning Services Configuration - This configuration allows access to any of the systems set up to provision users with services.

See Appendix A2 for the full text.

ISP1 Configuration - This configuration permits access to Service Provider system 1 (10.3.0.1).

See Appendix A3 for the full text.

2.6 Client Systems

The Consumer PCs used in the testing were all Windows/Intel- based systems. Standard Microsoft networking stacks were installed and all were configured with Microsoft Dial-up Networking v1.3. L2TP shims were from the iVasion WinVPN Client 1.11.

Telcordia Technologies, Unrestricted Access.
Copyright © Telcordia Technologies, Inc.

Win 95, IBM 755c, Intel 80486, 20MB.

WinNT 4.0, Dell Optiplex GxA, 64MB.

Win 98, Dell Latitude XP, Intel 80486, 16MB (yes, painfully slow!).

Telcordia Technologies, Unrestricted Access.
Copyright © Telcordia Technologies, Inc.

3 Test Plan Elements

The test cases generally follow the steps a Consumer would take to obtain service. Not all tests apply to all system configurations. Also, the process and procedures that are in place in a given AM/CNO installation may change slightly how a Consumer requests access and is ultimately connected to a ISP. Figure 12 illustrates the transitions.

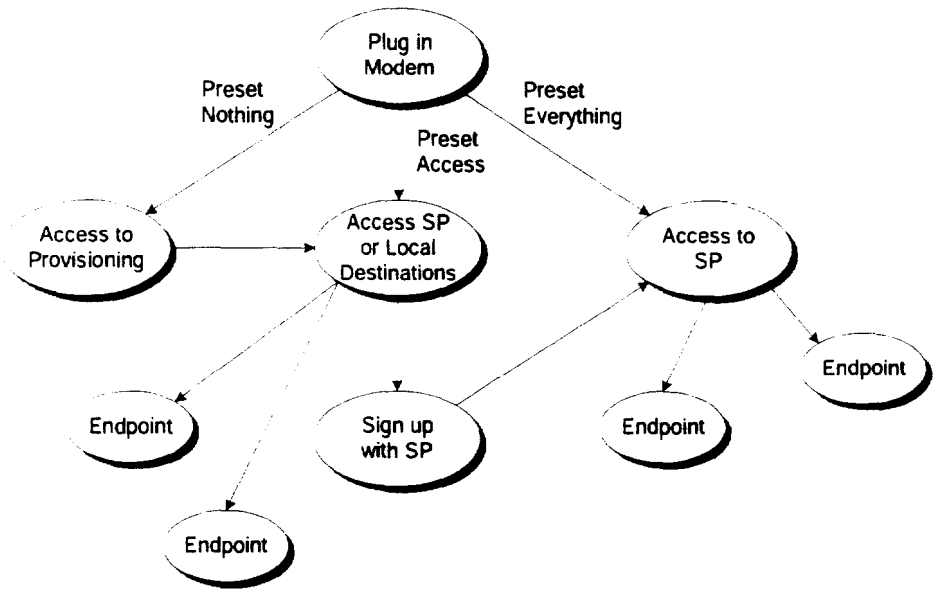

Figure 12 Consumer-ISP Access States

There are three possible sets of preconditions:

1) Nothing has been set up before the modem is inserted into the plant. In this case, the Consumer must be connected to a provisioning service that will provide the minimal access required to gain IP connectivity to other services.

2) The access has been set up. Here, the Consumer can gain IP access to the distribution network and the destinations that are allowed with simple access. These destinations include (possibly) local institutions (e.g. libraries, schools, etc.), and ISP's automated sign-up services.

3) Everything has been set before the modem is plugged into the plant. Here, the Consumer simply accesses the ISP they have chosen, and any other permitted destinations in the access network.

3.1 New Modem Permits Consumer PC IP Access

When a CM that is not associated with any consumer account or ISP is added to the network, it must be able to establish connectivity at the physical, MAC, and IP levels in order for any attached Consumer equipment to obtain services. **AOL(2)001808**

Setup:

Copyright © Telcordia Technologies, Inc.

SNMP tool for reading device and interface MIBs on CMTS and CM devices. Only read access to these components is necessary.

A Network Monitoring device or program to capture packet traces is useful to examine the exchange between the Consumer PC and the Network Services, ISPs, and headend interconnection.

It is always good to have several new CMs available for testing. Modems that have previously been inserted into the plant may have left traces of their presence and cause false readings to be taken.

The DHCP services should be configured with proper address pools to service CMs according to the system design.

Auto provisioning service or Modem-IP mapping made.

Consumer PC DHCP-enabled, set to acquire address.

3.1.1 New Modem Establishes Connectivity

When a new CM is added to the HFC network, it should quickly go through its synchronization phases, acquire downstream signal, listen to determine how to communicate on the upstream, and go through a ranging sequence to set its timing characteristics with the distant CMTS. This should occur without regard to the type of HFC or distribution network that is in place.

Objective: Ensure that CM establishes PHY and MAC synchronization with the CMTS it is connected to.

Procedure: Connect a CM that is not registered with any CMTS to the cable plant. Power the CM up by plugging the power supplies in to the appropriate power source.

Results: The modem should synchronize at the PHY and MAC levels. On some CMTS units, the CM will have its MAC address added to internal tables that indicate its state.

❒ Using the command appropriate for the CMTS, determine if the CM has connected and ranged properly.

Test Network	Results	
2.4.1	OK	All modems are able to synchronize and range. (MAC and PHY layer process)
2.4.2	OK	
2.4.3	OK	
2.4.4	OK	
2.4.5	OK	
2.4.6	OK	

AOL(2)001809

Copyright © Telcordia Technologies, Inc.

3.1.2 New CM Can Transmit IP Packets

Objective: Ensure that the CM is able to broadcast DHCP requests into the distribution network and the network services systems.

Procedure: Attach a traffic monitoring program or device to the Headend interconnect (or any point between the CM-CMTS and DHCP service) and record traffic as the modem synchronizes. If necessary, restart the CM so that it attempts to resync with the CMTS.

Results: The traffic monitor should capture DHCP DISCOVER packets that were broadcast from the CM. If the CMTS acts as a DHCP relay, its IP address should appear in the GIADDR field of the DISCOVER packets.

❒ Examine the capture log and determine that the DHCP DISCOVER packets from the CM are either unaltered by the CMTS or have appropriate GIADDR or relay options filled in properly.

Test Network	Results	
2.4.1	OK	Typical results in Section C1.
2.4.2	OK	
2.4.3	OK	
2.4.4	PPP encapsulation prevents PPPoE from being effective. Through tunneling with PPTP or L2TP are ok.	
2.4.5	OK	
2.4.6	OK	

3.1.3 New CM Receives Appropriate IP Address

The CM should receive an address that allows it to access the provisioning services. If the system is set up for automatic modem provisioning this address should permit access to the provisioning service without previous knowledge of the service. If the modem was required to be registered previously (e.g. its MAC address added to the system before it is recognized) the correct DHCP server should respond with an appropriate IP address.

Objective: Verify that CM receives address from either the " unknown modem" , " known, but unprovisioned" , or the " provisioned and ready" address pool. Also, that the correct DHCP server has responded.

Procedure: Examine the capture log of the DISCOVER-OFFER-REQUEST-ACK sequence that the modem went through. Also, examine the docsIfCmtsCmStatusTable to determine the CM MAC to IP address mapping.

AOL(2)001810

Copyright © Telcordia Technologies, Inc.

Results: The traffic monitor should have captured a complete DHCP sequence that shows that the correct DHCP server responded, and that the address is appropriate for the new CM. The CMTS should have the correct MAC address to IP address binding in the table of the CMTS. The DHCP OFFER should contain the following fields:

- ❒ Note the address of the correct DHCP server.
- ❒ Ensure that the DHCP OFFER is properly constructed.
- ❒ Verify the modem has a correct IP address.

Test Network	Results	
2.4.1	OK	Typical results in Section C1. Server: 10.2.0.2 (No pooling is available on DHCP server in use. All unknown modems receive address from default scope value.)
2.4.2	OK	
2.4.3	OK	
2.4.4	OK	
2.4.5	OK	
2.4.6	OK	

3.1.4 CM Received Correct Configuration File

A key parameter delivered in the DHCP OFFER is the address of the TFTP server used to send out modem configuration files, and the name of a file to download.

Objective: Ensure that CM received appropriate modem configuration file.

Procedure: Examine the capture log of the DISCOVER-OFFER-REQUEST-ACK sequence to examine the " file" and " server" parameters of the OFFER. Use SNMP to examine the docsDevServerTftp and docsDevServerConfigFile variables.

Results: The capture sequence that was acknowledged should have the filename and server address of the TFTP service appropriate for the modem. The CM should have values in its MIB that identify its configuration file.

- ❒ Note the address of the server and the name of the configuration file that was loaded into the modem.

Test Network	Results	
2.4.1	OK	Server: 10.2.0.2 Either default file for scope or file assigned to address reservation.
2.4.2	OK	
2.4.3	OK	
2.4.4	OK	
2.4.5	OK	

Copyright © Telcordia Technologies, Inc.

2.4.6	OK	

3.1.5 Consumer PC Obtains Appropriate IP address

After the CM has established IP connectivity, the Consumer PC will be allowed to pass traffic. The Consumer PC must acquire an address that allows it to access the provisioning services of the AM. If the system is set up for unattended provisioning, then there will be some server-side application (HTTP server or specialty application) that the Consumer PC will contact to effect this.

Objective: Ensure that PC receives IP address appropriate for access to service provisioning servers.

Procedure: Examine the PC IP stack to verify the address that the PC has. Examine any IP filtering configurations or Access Control Lists in intervening network elements to ensure that the path to the provisioning service is clear.

Results: The PC should have an address that allows it to access the provisioning servers. No IP packet filters can be set in the CM, CMTS, or any network element between the Consumer PC and the provisioning servers that would deny the PC access to the server or service.

❒ Note the addresses of the Consumer PC and the provisioning servers.

❒ Verify that there are no packet filters that would hinder access to the provisioning service (attempt to access the service, next test).

Test Network	Results	
2.4.1	OK	Typical sequence in Section C2. (DHCP relay agent 10.12.0.1)
2.4.2	OK	
2.4.3	N/A PC addresses were assigned and hand configured.	
2.4.4	OK	
2.4.5	N/A PC addresses were assigned and hand configured.	
2.4.6	OK	

3.2 Consumer Selects ISP

Once the Consumer PC has been configured properly and has IP access to the distribution network it should be able to access the provisioning servers. The first step may be to register with the AM if the service provisioning model is of the zero-knowledge type. If already registered with the AM the Consumer PC should have access to the provisioning servers of the ISPs and should be able to run whatever software is necessary to sign up for services.

AOL(2)001812

Copyright © Telcordia Technologies, Inc.

Setup:

Client side software set up.

Consumer PC has access to the distribution network.

3.2.1 Consumer PC Reaches Configuration Services

A system design that requires the Consumer to have registered offline with a ISP may only need to verify that they are indeed a valid user of the service.

Objective: Verify that Consumer PC is able to access configuration service.

Procedure: Launch the client-side provisioning access application (custom app or Web browser) with the appropriate access configuration in place. Go to the registration or sign-up page and attempt to register for services.

Results: A consumer that must go to a service provisioning or registration server should be able to easily access the server and sign up for services offered.

❒ Verify that the Consumer PC is able to access provisioning servers in the distribution network.

❒ Verify that a properly configured client-side application is able to access the provisioning service of each service provider.

Test Network	Results
2.4.1	OK
2.4.2	OK
2.4.3	By default, the PC was hand-configured to be in the ISP network.
2.4.4	OK
2.4.5	By default, the PC was hand-configured to be in the ISP network.
2.4.6	OK

3.2.2 Consumer PC Only accesses Configuration Services

A Consumer PC that has IP connectivity to the distribution network will be able to exchange traffic with permitted destinations without registering with a ISP. These destinations may be limited to the AM server that is used to sign users up for services. Or it may include local institutions (e.g. libraries, schools) if there is an access-only service in place. Either way, once the Consumer PC has attained connectivity, it must only exchange traffic with allowed destinations.

Objective: Verify that PC is unable to access other services or ISPs while connected to the Provisioning Service.

AOL(2)001813

Copyright © Telcordia Technologies, Inc.

Procedure: List destinations that are not allowed without Consumer-AM-ISP agreement. After the CM has attained IP connectivity and the PC is permitted to pass traffic, attempt to access these nodes both inside and outside the Distribution network.

Procedure: List destinations that are allowed. Attempt to exchange traffic with those.

Results: The Consumer PC should be able to exchange traffic with permitted destinations, and should not be able to exchange traffic with not-permitted destinations.

❒ Verify that a connected consumer PC is only permitted to access allowed destinations.

❒ Verify that a connected consumer PC cannot access destinations not allowed without a service agreement in place.

Test Network	Results	
2.4.1	OK	Filters in CMs keep PCs in their own space.
2.4.2	OK	
2.4.3	OK	
2.4.4	OK	
2.4.5	OK	
2.4.6	OK	

3.2.3 CM Reset Necessary for PC Access

Many service provisioning processes will require that the CM be reset after the Consumer has signed up for a ISP. This will be the case if the unassigned Consumer has been herded into a provisioning server or a sandbox area that permits limited access to destinations on the distribution network. The reset could be a soft reset issued by the provisioning service (setting docsDevReset), or a hard reset by depowering or pressing a reset button.

Objective: Verify that the service-enabled PC is unable to access services, until the CM has been reset.

Procedure: After the Consumer has selected a ISP, but before the CM has been reset, attempt to access the destinations from Section 3.2.2. If the reset is soft, from an automated provisioning service, block it until the test is finished. If the reset is hard, simply delay the reset until the test is finished.

Results: The Consumer PC should be able to access only allowed destinations after signing up for a service. The Consumer PC should be in the same state as Section 3.2.2.

❒ The Consumer PC is not able to access unavailable destinations before reset.

Test Network	Results

AOL(2)001814

Copyright © Telcordia Technologies, Inc.

2.4.1	OK	Reset to reboot modem and acquire a new configuration. (No CMTS-based controls are in place.) In Policy-routed configurations, necessary to include policy information in routers.
2.4.2	OK	
2.4.3	OK	
2.4.4	OK	
2.4.5	OK	
2.4.6	OK	

3.2.4 CM Receives Proper Configuration After Reset

After the Consumer has selected a ISP, it may be necessary for their cable modem to receive a configuration file (from the TFTP service) that reflects that selection. The file will specify the transport services the modem will receive and possibly contain filters that limit access to selected destinations throughout the AM/CNO distribution network.

Objective: Determine that a properly signed-up consumer PC is able to access its service provider when the CM has been reset.

Procedure: Reset the Consumer CM by setting docsDevReset. Then attempt to access the chosen ISP. Reset the Consumer CM by depowering (completely remove power from the power outlet, some CMs continue network connectivity when the power switch is turned off).

Results: The CM should go through its bootstrapping sequence, which includes requesting a set of network parameters from the DHCP server and a configuration file from the TFTP server. The address should be correct for the service that the consumer has signed on with. The configuration file that the CM receives should be correct for the service.

❒ The CM has acquired the correct IP address.

❒ The CM has downloaded the correct configuration file.

Test Network	Results	
2.4.1	OK	Yes, The entry for the CM (Key is MAC address) in DHCP was set to deliver the proper configuration file. Policy Configurations need policies distributed.
2.4.2	OK	
2.4.3	OK	
2.4.4	OK	
2.4.5	OK	
2.4.6	OK	

3.3 Tunnel Solutions

The requirements state that the AM must separate traffic destined for different ISPs. One important technique for accomplishing this is to use

Telcordia Technologies, Unrestricted Access.
Copyright © Telcordia Technologies, Inc.

tunnels at layer 2 or layer 3. The tunnel permits the consumer to access the chosen ISP's network, but nothing else.

The CM connected to the Consumer PC is configured to only allow access to the network services system msoNT and the tunnel server. When the CM bootstraps it receives a non-routable address. The CMTS acts as a DHCP relay and the DHCP server (msoNT) sees a directed request from that network element. Lease renewals are directed to the server from the CM. Likewise, the PC receives a non-routable address, and the CMTS acts as a DHCP relay. The user executes Dial-up Networking and selects the Tunnel Server they need to contact. The configuration from the server includes a routable address which allows the PC to access services beyond the tunnel endpoint and access the greater Internet in a normal fashion.

3.3.1 Consumers Access Only Permitted Tunnels

The Consumer PC should only be able to access destinations that are allowed in day-to-day use. These include the tunnel servers of their chose ISP and other destinations located within the AM/CNO network that are permitted with the access service (could be none).

Objective: Verify that PC is only able to access tunnel services of selected provider.

Procedure: Initiate a session with the chosen ISP. Create a list of destinations that should not be permitted access and attempt to exchange traffic with those destinations.

Results: The Consumer PC should only be able to access the chosen service provider and any other destinations within the AM/CNO distribution network that are permitted by their subscription.

❒ The Consumer PC is able to access only allowed destinations.

Test Network	Results	
2.4.1	OK	All traffic delivered through the ISP. Local references too. Filters block access to forbidden destinations if the user attempts to override normal routing.
2.4.2	OK	
2.4.3	N/A	
2.4.4	OK	
2.4.5	N/A	
2.4.6	OK	

3.3.2 Consumer PC Can Establish Tunnel Endpoint

An access network that uses tunneling techniques to separate Consumer traffic must permit tunnel set-up messages to flow from the Consumer PC to the tunnel server of the chosen ISP.

Objective: Ensure that PC is able to establish a tunnel to the chosen ISP tunnel server.

AOL(2)001816

Copyright © Telcordia Technologies, Inc.

Procedure: Launch the tunnel endpoint program on the Consumer PC (e.g. Dial-up-networking on Windows platforms). Ensure it is properly configured to connect to the chosen ISP tunnel server. Use the client-side tunnel endpoint program to access the chosen ISP tunnel server.

Results: The Consumer PC should be able to connect to the tunnel server of their chosen ISP.

❒ Note the IP address of the tunnel server being contacted.

❒ Note the type of tunnel being established and the software in use on the client-side.

❒ The Tunnel connection was successful.

Test Network	Results	
2.4.1	OK	10.3.0.1, PPTP, MS Dial-up NW 10.8.0.1, L2TP, iVasion Client over MS DUN.
2.4.2	OK	
2.4.3	N/A	
2.4.4	OK	
2.4.5	N/A	
2.4.6	OK	

3.3.3 Consumer PC receives Correct ISP Configuration

The Consumer PC should receive an IP address, subnet mask, name server address, and other network configuration parameters from the chosen ISP. This permits the PC to properly act as a client within the Tunnel network.

Objective: Ensure that the Consumer PC has received proper configuration from ISP.

Procedure: Connect to the ISP tunnel server. Use the ipconfig or winipcfg command to examine the IP configuration currently held by the PC IP stack.

Results: The IP stack on the Consumer PC should have a set of valid IP configuration parameters that were obtained from the ISP tunnel service.

❒ Verify the IP configuration on the Consumer PC communications stack.

Test Network	Results	
2.4.1	OK	Needed to preset by hand the DNS server addresses.
2.4.2	OK	
2.4.3	N/A	
2.4.4	OK	
2.4.5	N/A	

AOL(2)001817

Copyright © Telcordia Technologies, Inc.

2.4.6	OK	

3.3.4 Consumer PC Exchanges Traffic with Chosen ISP

When properly configured and connected, the Consumer PC should be able to exchange traffic with the chosen ISP.

Objective: Test that the Consumer PC is able to access all services contracted for in the ISP network.

Procedure: Using appropriate client-side applications, access each service that the ISP provides to the Consumer. Upload and download several objects such as Usenet News and e-mail messages, and web pages. If other, specialty applications are available (e.g. Net Radio) access these services.

Results: The Consumer PC should be able to access all available services.

❒ Ensure that properly connected PC is able to pass traffic to ISP network and access services.

Test Network	Results
2.4.1	OK
2.4.2	OK
2.4.3	N/A
2.4.4	OK
2.4.5	N/A
2.4.6	OK

3.4 Policy Router Solutions

Policy router-based system designs aggregate all traffic flows into a single distribution point at which all ISPs have a connection. Packets are distributed and routed only from the policy router. The important difference with other designs is that after Consumer service-bound packets are delivered to the policy router, it uses some characteristics of the packets to determine which ISP network rather than destination address.

3.4.1 Consumer PC receives Correct ISP Configuration

Verify that Consumer PC has received proper configuration from ISP.

The Consumer PC should receive an IP address, subnet mask, name server address, and other network configuration parameters from the chosen ISP. This permits the PC to properly act as a client within the Tunnel network.

Objective: Ensure that the Consumer PC has received proper configuration from ISP. **AOL(2)001818**

Copyright © Telcordia Technologies, Inc.

Procedure: Connect to the ISP tunnel server. Use the ipconfig or winipcfg command to examine the IP configuration currently held by the PC IP stack.

Results: The IP stack on the Consumer PC should have a set of valid IP configuration parameters that were obtained from the ISP tunnel service.

❒ Verify the IP configuration on the Consumer PC communications stack.

Test Network	Results
2.4.1	N/A
2.4.2	N/A
2.4.3	Hand configured to appropriate ISP
2.4.4	N/A
2.4.5	Hand configured to appropriate ISP
2.4.6	N/A

3.4.2 Consumer PC Exchanges Traffic with Chosen ISP

Ensure that properly connected PC is able to pass traffic to ISP network.

When properly configured and connected, the Consumer PC should be able to exchange traffic with the chosen ISP.

Objective: Test that the Consumer PC is able to access all services contracted for in the ISP network.

Procedure: Using appropriate client-side applications, access each service that the ISP provides to the Consumer. Upload and download several objects such as Usenet News and e-mail messages, and web pages. If other, specialty applications are available (e.g. Net Radio) access these services.

Results: The Consumer PC should be able to access all available services.

❒ Ensure that properly connected PC is able to pass traffic to ISP network and access services.

Test Network	Results
2.4.1	N/A
2.4.2	N/A
2.4.3	OK
2.4.4	N/A
2.4.5	OK
2.4.6	N/A

AOL(2)001819

Copyright © Telcordia Technologies, Inc.

3.4.3 Consumers Access Only Permitted Destinations

Ensure that PC of one ISP is able to access others in same transport subnet only through ISP.

The Consumer PC should only be able to access destinations that are allowed in day-to-day use. These include the tunnel servers of their chose ISP and other destinations located within the AM/CNO network that are permitted with the access service (could be none).

Objective: Verify that PC is only able to access tunnel services of selected provider.

Procedure: Initiate a session with the chosen ISP. Create a list of destinations that should not be permitted access and attempt to exchange traffic with those destinations. Use a traceroute program to determine the path taken to the destinations.

Results: The Consumer PC should only be able to access the chosen service provider and any other destinations within the AM/CNO distribution network that are permitted by their subscription.

❒ The Consumer PC is able to access only allowed destinations.

Test Network	Results
2.4.1	N/A
2.4.2	N/A
2.4.3	OK
2.4.4	N/A
2.4.5	Users from different ISPs, arriving on same interface from a bridged subnet were able to exchange traffic at the inbound interface.
2.4.6	N/A

AOL(2)001820

Copyright © Telcordia Technologies, Inc.

4 Requirements/Test Summary

The following Table summarizes the test results for the six network configurations, and for the 11 requirements that were identified in the companion document " Implementing Open Access Over Cable Systems - A Technical Perspective" [OpenTech].

	Network 1	Network 2	Network 3	Network 4	Network 5	Network 6
Req 1	OK	OK	OK	OK	OK	OK
Req 2	OK	OK	OK	OK	OK	OK
Req 3	OK	OK	OK	OK	OK	OK
Req 4	OK	OK	Note 1	OK	Note 2	OK
Req 5	OK	OK	OK	OK	OK	OK
Req 6	OK	OK	OK	OK	OK	OK
Req 7	OK	OK	OK	OK	OK	OK
Req 8	N/A	N/A	OK	OK	OK	OK
Req 9	N/A	N/A	OK	N/A	Note 3	N/A
Req 10	Note 4	Note 4	OK	Note 4	OK	Note 4
Req 11	N/A	N/A	N/A	N/A	N/A	N/A

Note 1 - Multiple addresses needed to be assigned to headend interconnect interface. Redback AOS before 3.1 did not permit multiple address assignment (secondary IP address) to single interfaces; multiple physical ports with different addresses hubbed to provide multiple ISP address blocks.

Note 2 - Subnets need to be created at CMTSs to support each ISP; routing tables need to be maintained to support multiple address spaces. Users from different ISPs arriving at common interface from a bridged CMTS (albeit different address spaces) are able to exchange traffic.

Note 3 - Multiple router hops, policy set in each.

Note 4 - Tunnel causes loss of lease for NIC in PC. Need to extend PC lease indefinitely.

Table 2 Requirements Summary

The experimental measurements summarized in Table 2 confirm the successful technical demonstration of an Equal Access model using six

Telcordia Technologies, Unrestricted Access.
Copyright © Telcordia Technologies, Inc.

different network configurations and five equipment vendors, with existing DOCSIS standard and off-the-shelf capabilities.

4.1 Conclusion

We evaluated several architectures that would facilitate open and equal access over cable networks. Policy-based routing requires much configuration and incurs continuing operational overhead for policy distribution and address space management. PBR would be applicable for small operators with a simple bridged distribution network that has a single aggregation point at which all ISPs connect. This simplifies the policy implementation. However, address space management issues will dominate the operational overheads. Multiple ISP households would be complicated for both Access Managers and Consumers to manage.

Tunneling at Layer 2 (PPPoE) is an alternative for the small operator with a bridged network. It requires less management overhead, but in its current form, requires authentication and authorization decisions to be made from the network element that terminates the connections.

IP tunneling over IP transport (PPTP, and L2TP) is the best choice across all system designs. It permits the Access Manager to create simple addressing plans based on non-Internet routable address spaces. Consumer address space management is given to the ISPs for them to manage as part of their service. It gives AMs flexibility in where to interconnect with the ISPs so long as the ISP Points-of-interconnection are directly connected to the AM network. Authentication and authorization decisions can be made on an end-to-end basis by the ISPs. Multiple ISP households are easy to accommodate by simply adding multiple destinations to the Consumer's configuration.

Telcordia Technologies, Unrestricted Access.
Copyright © Telcordia Technologies, Inc.